AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for encrypting data, the method comprising:

providing a first data processing system for a first user ~~including the first user's private key and a master private key;~~and a second data processing system for a second user;

~~providing a second data processing system for a second user including program instructions and the first user's public key and master public key to generate a session key, to encrypt original data using the session key, to encrypt the session key with the first user's public key, to encrypt the session key with the master public key, to generate a first data packet including a plurality of encrypted session keys and encrypted data, and to transmit the first data packet to one or more different data processing systems instead of or in addition to the first data processing system; and~~

~~the first data processing system receiving the first data packet and including program instructions to decrypt one of the encrypted session keys with the private key of the first user, and to decrypt the encrypted data with the session key to re-create the original data.~~

providing a session key randomly generated by the second system for use in encrypting original data;

encrypting the data using the session key and a symmetric encryption routine;

encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob;

encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob;

storing a first user private key on any media;

decrypting the user key blob using the asymmetric encryption routine providing the first system with access to the session key; and

the first system decrypting the data using the symmetric encryption routine and securely transmitting the data to the first system.

2. – 6. (Canceled)

7. (Currently Amended) The method, as set forth in claim 1, further comprising storing the first user's private key on a data storage medium coupled to ~~the~~ a destination data processing system.

8. (Previously Presented) The method, as set forth in claim 1, further comprising storing the master private key on a data storage medium coupled to the destination data processing system.

9. (Currently Amended) The method, as set forth in claim 7, further comprising retrieving the first user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

10. (Currently Amended) The method, as set forth in claim ~~1~~7, further comprising retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

11. (Original) The method, as set forth in claim 1, further comprising utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

12. (Currently Amended) A method for encrypting data comprising:

providing a first data processing system for a first user ~~including the first user's private key and a master private key;~~ and a second data processing system for a second user;

~~providing a second data processing system for a second user including program instructions and the first user's public key and a master public key to generate a session key, to encrypt original data using the session key, to encrypt the session key with the first user's public key, to encrypt the session key with the master public key, to generate a first data packet including a plurality of encrypted session keys and encrypted data,~~

~~and to transmit the first data packet to one or more different data processing systems instead of or in addition to the first data processing system;~~

~~the first data processing system receiving the first data packet and including program instructions to decrypt one of the encrypted session keys with the private key of the first user, and to decrypt the encrypted data with the session key to re-create the original data; and~~

~~the master public key and the master private key allowing another user to gain access to encrypted data, the other user executing program instructions on the first data processing system to decrypt the one encrypted session key using the master private key, and to decrypt the encrypted data with the session key to re-create the original data.~~

providing a session key randomly generated by the second system for use in encrypting original data;

encrypting the data using the session key and a symmetric encryption routine;

encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob;

encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob;

storing a first user private key on any media;

decrypting the user key blob using the asymmetric encryption routine providing the first system with access to the session key; and

the first system decrypting the data using the symmetric encryption routine and securely transmitting the data to the first system and;

a third party gaining access to the data using a master private key to decrypt the master key blob using the asymmetric encryption routine and gain access to the original data.

13.–17.(Canceled)

18. (Currently Amended) The method as set forth in claim 12, wherein the first user's private key is stored on a data storage medium coupled to the second data processing system.

19. (Previously Presented) The method as set forth in claim 12, wherein the master private key is stored on a data storage medium coupled to the second data processing system.

20. (Currently Amended) The method as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the first user's private key from a smart card.

21. (Previously Presented) The method as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the master private key from a smart card.

22. (Previously Presented) The method as set forth in claim 12, further comprising:

a plurality of master private keys; and

a plurality of master public keys.

23.–29.(Canceled)

30. (New) A method for encrypting data comprising:

providing a first data processing system for a first user and a second data processing system for a second user;

the second user sending the first user a data file;

the second system randomly generating a session key for use in encrypting original data in the data file;

using the session key, the second system encrypting the data using a symmetric encryption routine;

encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob within the encrypted data;

encrypting the session key with a master public key using the asymmetric encryption routine, for storage as a master key blob within the encrypted data;

transmitting the encrypted data to the first system;

storing a first user private key on any media;

decrypting the user key blob using the asymmetric encryption routine providing the first system with access to the randomly generated session key;

the first system decrypting the data using the symmetric encryption routine and securely transmitting the data to the first system; and

a third party gaining access to the data using a master private key to decrypt the master key blob using the asymmetric encryption routine and gain access to the original data.